REMARKS

This Amendment is in response to the Office Action dated February 25, 2009 (the Action).

The Action objects to the Specification on page 2. The Action rejects Claims 1-3 and 9-20 under 35 U.S.C. 102(a) as being anticipated by EP 1361527 to Anderson (Anderson). Claims 4-8 and 21-25 stand rejected under 35 U.S.C. 103(a) as being unpatentable over Anderson in view of U.S. Patent No. 6,760,912 to Yarsa (Yarsa).

It is noted that Claims 26-35 are discussed in the Action on pages 3-5 in the 35 U.S.C. 102(a) rejections. However, Claims 26-35 are not identified in the rejection under 35 U.S.C. 102(a) on page 2 of the Action. Applicants will treat Claims 26-35 as also being rejected in the Action under 35 U.S.C. 102(a) as discussed on pages 3-5 of the Action for purposes of this amendment and response. Clarification is respectfully requested.

The independent Claims 1, 14, 18 and 31 have been amended above to clarify that the an object includes access permissions and other permission information to be associated with policy contained in the downloaded object as well as access permissions already existing in the apparatus, and the object includes new routines and/or new functions. The independent Claims 1, 14, 18 and 31 further recite that the object enhances the application interface with the new routines and/or new functions. Support for the above amendments can be found, for example, in the Specification on page 3, paragraph [0059].

Applicants respectfully request reconsideration in view of the above amendments and the remarks that follow.

I. <u>The Objections to the Specification</u>

Applicants have amended the Specification above to address the informalities noted on page 2 of the Action. Accordingly, Applicants request that the objections to the Specification be withdrawn.

II. <u>The Independent Claims 1, 14, 18 and 31</u>

Claim 1 recites as follows:

> A method of providing a dynamic security management in an apparatus, the apparatus comprising: a platform for running an application; a security manager for handling access of the application to functions existing in the apparatus; an application interface between the platform and the application; a set of access permissions stored in the apparatus and used by the security manager for controlling access of the applicationto functions through the application interface the method comprising:
>
> downloading into the apparatus an object containing access permissions and other permission information to be associated with policy contained in the downloaded object as well as access permissions already existing in the apparatus, wherein the permissions are applicable to at least one function, the object comprising new routines and/or new functions;
>
> verifying the object; and
>
> installing the access permissions together with the existing permissions, the object enhancing the application interface with the new routines and/or new functions.

Anderson proposes a method for loading an application in a device. In order to operate in the device, the application in Anderson apparently needs access to functions of the device. The application's access to functions of the device is controlled through an interface unit API governed by access rights. In Anderson, the access rights are defined by preloaded attribute certificates. The access rights control what functions may be accessed by the application. *See* Anderson, paragraphs [0020]-[0021].

However, Anderson is silent about any sharing of the downloaded application. In other words, it appears that the downloaded application of Anderson may not be used by other applications and functions of the device. Applicants submit that Anderson does not make any provisions for controlling access to the downloaded application, and the preloaded attribute certificates of Anderson do not appear to contain such access rights.

Applicants submit that the access rights that are defined by *preloaded* attribute certificates in Anderson do not disclose or render obvious the recitations of Claim 1. For example, Anderson does not disclose that a downloaded *object* includes *access permissions* and other permission information to be associated with policy contained *in the downloaded object* as well as access permissions already existing in the apparatus.

In contrast to Anderson, embodiments according to the present invention relate to objects that may be shared, *i.e.*, accessed by functions and applications that are already downloaded, or to be downloaded in the future. *See* Specification, page 3, paragraph [0059]. Accordingly, the access rights to the downloaded objects are controlled. Thus, the control of access rights to the downloaded object is controlled by including permission information to be associated with the policy contained in the downloaded object. Thus, the downloaded object includes permissions related to the object itself. Since an API is generally defined by its access rights, the API will be controlled dynamically because, according to embodiments of the invention, access permissions may be downloaded in a secure manner. Thus, the downloaded object can enhance the application interface so that new routines and/or new functions may be downloaded and shared with applications that are already downloaded or that will be downloaded in the future. These potential advantages are not appreciated by the preloaded attribute certificates of Anderson.

Accordingly, the access rights that are defined by *preloaded* attribute certificates in Anderson do not disclose or render obvious the recitations of Claim 1, *i.e.*, that the downloaded *object* includes *access permissions* and other permission information to be associated with policy contained *in the downloaded object* as well as access permissions already existing in the apparatus.

These recitations are also not disclosed or rendered obvious by Yarsa, which is cited with respect to Claims 4-8 and 21-25.

Accordingly, Applicants submit that Claim 1 is not disclosed or rendered obvious by the cited prior art. Claims 14, 18 and 31 include recitations analogous to those discussed above and are likewise patentable over the cited prior art. Claims 2-13, 15-17, 19-30 and 32-35 depend from Claims 1, 14,18 and 31, respectively, and are patentable at least per the patentability of the claims from which they depend. Applicants respectfully request that the rejections be withdrawn.

CONCLUSION

Accordingly, Applicants submit that the present application is in condition for allowance and the same is earnestly solicited. Should the Examiner have any matters outstanding of resolution, he is encouraged to telephone the undersigned at 919-854-1400 for expeditious handling.

Respectfully submitted,

Laura M. Kelley
Registration No.: 48,441

USPTO Customer No. 20792
Myers Bigel Sibley & Sajovec
Post Office Box 37428
Raleigh, North Carolina 27627
Telephone: 919/854-1400
Facsimile: 919/854-1401

CERTIFICATION OF TRANSMISSION

I hereby certify that this correspondence is being transmitted via the Office electronic filing system in accordance with § 1.6(a)(4) to the U.S. Patent and Trademark Office on May 26, 2009.

Signature: Joyce Paoli
Joyce Paoli